

REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants wish to thank the Examiner for the thorough examination and search of the subject.

Claims 33, 64, and 67 are amended.

Claim 64 is amended to remove the term, “electrical” from line 7. There was insufficient antecedent basis for this term in the claim.

Claims 1-12, 19-21, 24, 27, 33-39, 45-47, 50, 53, 59-61, and 64-73, stand rejected under 35 U.S.C 102(b) as being anticipated by Fisherman et al (USP 5,586,301). The Fisherman reference is directed to a personal computer hard disk protection system. The system comprises protection programs that interpret logical drives of the hard disk as a fixed set of zones for a particular user wherein each of the fixed set of zones each has respective access rules. The system includes a hardware module (PPSM) responsive to the protection programs and operable to allow or deny access to the hard disk based on the access rules. Fisherman et al do not teach or suggest, among other things, determining if an access request is a security risk, determining the state of a switch, and determining whether to execute a determined security risk access request based on a determined switch state. Fisherman et al also do not teach or suggest including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of an interface control command by the interface controller depending on whether or not the source of the interface control command is authentic.

Applicant’s claimed invention, as recited in independent Claims 1, 64, and 70, is directed to protecting computer assets from unauthorized access. Applicant clearly teaches determining if an interface control command is a security risk and, if so, then determining the state of a switch.

The interface control command that is identified as security risk is then either inhibited or executed *based on the determined state of the switch* (See, for example, Claim 1, lines 5-11). The cited portion of Fisherman et al is silent on determining the state of a switch and on using a switch state to further determine whether to allow or to disallow a hard drive access request that is known to violate an access rule. Where Fisherman et al detect an access request that violates an access rule, this access operation is simply not performed and an error code is returned. The disposition of the violating access request does not depend on a determined switch state (See, for example, column 6, line 62 through column 7, line 2). Therefore features of Applicant's claimed invention are not taught or suggested by Fisherman et al. Accordingly, independent Claims 1, 64, and 70 are allowable, and the dependent claims add additional novel and non-obvious subject matter and should likewise be allowable.

If a rejection is maintained, Applicant respectfully requests a showing from the Examiner where Fisherman et al actually teach all the features of Applicant's claimed invention and, in particular, determining if an access request is a security risk, determining a switch state, and then determining whether to execute a determined security risk access request based on a determined switch state.

Applicant's claimed invention, as recited in independent Claims 33 and 67 is directed to protecting computer assets from unauthorized access. Applicant clearly teaches receiving an interface control command in a protection engine *in a south bridge*. The security risk of the interface control command is determined. If the interface control command is determined to be a security risk, then the source of the command is authenticated. An interface control command that is a determined security risk is then inhibited or executed based on whether or not the source of the command is authentic (See, for example, Claim 33, lines 3-10). In Claim 67, Applicant

teaches *a south bridge* comprising an interface controller and a protection engine operable to determine if a source of an interface control command is authentic and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. (See Claim 67, lines 3-11). Most particularly, the cited portion of Fisherman et al is silent on receiving an interface control command in a protection engine in a south bridge and on a south bridge comprising an interface controller and a protection engine operable to authenticating interface control commands. There is no discussion in Fisherman et al of a protection engine in a south bridge or of a protection engine and an interface controller in a south bridge. Therefore features of Applicant's claimed invention are not taught or suggested by Fisherman et al. Accordingly, independent Claims 1, 64, and 70 are allowable, and the dependent claims add additional novel and non-obvious subject matter and should likewise be allowable. If a rejection is maintained, Applicant respectfully requests a showing from the Examiner that Fisherman et al actually teach all the features of Applicant's claimed invention and, in particular, including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic.

Claims 13-17, 28-32, 40-44, and 54-58, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al in view of Glossary of Information Technology Acronyms and Terms (here within GITAT). In regards to Claims 13-17, 28-32, 40-44, and 54-58, Applicant references the relevant remarks above. The GITAT reference provides cursory definitions of system input-output (I/O) terms. The GITAT reference does not teach or suggest either (1) determining if an access request is a security risk, determining a switch state, and then

determining whether to execute a determined security risk access request based on a determined switch state or (2) including in a south bridge a protection engine operable to authenticating interface control commands. Furthermore, Fisherman et al teach protecting only a hard disk and further state that access “requests addressed to a floppy disk are not processed by the system 20, but are sent to the original disk-request handler 38 of INT 13H BIOS” (See, for example, column 11, line 65 through column 12, line 1). In light of this, it is not logical to suggest that Fisherman et al hint or suggest protecting assets other than the hard disk. Further yet, the cursory definitions of terms provided in GITAT provide no hint or suggestion for protecting assets other than hard drives. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 18, 25, 26, 51, and 52, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al and GITAT as applied to Claims 1 and 13 above, and further in view of Davis (USP 6,205,547). In regards to Claims 18, 25, 26, 51, and 52, Applicant references the relevant remarks above. Davis is directed to a computer managing system. However, Davis does not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 22, 23, 48, and 49, stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al in view of Chen et al (USP 5,832,208). In regards to


Claims 22, 23, 48, and 49, Applicant references the relevant remarks above. Chen et al is directed to an anti-virus software agent. However, Chen et al do not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Claims 62 and 63 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Fisherman et al in view of Applied Cryptography 2nd Edition (here within AC). In regards to Claims 62 and 63, Applicant references the relevant remarks above. AC is directed to an anti-virus software agent. However, AC does not teach or suggest either (1) determining if an access request is a security risk and then determining whether to execute the access request based on a switch state or (2) including in a south bridge a protection engine operable to authenticating an interface control command and to selectively allow or inhibit execution of the interface control command by the interface controller depending on whether or not the source of the interface control command is authentic. Accordingly, the dependent claims add additional novel and non-obvious subject matter and should be allowable.

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. Applicant respectfully reasserts remarks in response to the previous office action. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

Date: 4/3/06

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz, P.C.
222 N. LaSalle Street
Chicago, IL 60601
(312) 609-7500
FAX: (312) 609-5005